21 Mars 2019

Les cybermenaces et la communauté internationale

Par Ashley Taylor

Ce document fait état d'éléments de preuves de plus en plus nombreux de l'utilisation par la Corée du Nord (RPDC) des technologies numériques qui, si ce n'est déjà fait, pourraient devenir un outil puissant pour contourner les sanctions imposées par l'ONU. Grâce à ce résumé des violations constatées via l'utilisation de technologies informatiques et numériques avancées, les responsables de la mise en œuvre des sanctions et de la conformité apprendront à reconnaître, à préparer et à protéger les tentatives nord-coréennes visant à empiéter sur leurs systèmes de traitement de l'information, financier et commercial. Cette recherche ouvre également la voie à des recommandations de solutions possibles politiques, réglementaires et individuelles contre les menaces existantes et les fragilités futures.

Les abus de la RPDC dans la sphère numérique sont bien répertoriés. Ils comprennent les intrusions «traditionnelles» d'institutions financières, telles que les attaques par déni de service (DDOS), l'insertion de logiciels malveillants et les tentatives de phishing pour voler des fonds. De nouvelles preuves suggèrent également un effort concerté afin de développer des capacités technologiques pour des violations encore plus sophistiquées, y compris sur des plateformes numériques supposées des plus fiables telles que les échanges de crypto-monnaie. Ces attaques constituent la preuve d'un arsenal exotique d'armes numériques utilisées pour menacer la cyber sphère mondiale, voler de la crypto monnaie, détourner des actifs appartenant à des parties légitimes, et créer de fausses campagnes de financement pour de nouveaux actifs de crypto-monnaie, notamment par l'émission de Initial Coin Offerings (ICO). La RPDC peut ainsi s'appuyer sur sa réputation culturelle d'élite associée au piratage informatique et

Rico Carisch
rico.carisch@comcapint.com
+1-610-390-9541

www.comcapint.com
110 West 94 Street – 2D
New York, NY 10025

Loraine Rickard-Martin
loraine.rickard-martin@comcapint.com
+1-917-715-2142

l'encourager davantage grâce à de nouveaux outils pour le piratage des monnaies numériques.[1]

Le terrain numérique naissant

Les crypto-monnaies sont des logiciels qui permettent à quiconque de créer une nouvelle devise avec des règles spécifiques pour son offre, sa demande, son utilisation et son échange. Le logiciel est basé sur une nouvelle architecture connue sous le nom de technologie de registre distribué ou blockchain, qui fait référence à la manière dont les actions ou les transactions de crypto-monnaies sont regroupées dans des blocs enregistrés comme une chaîne d'événements. Outre la création de monnaies cryptées, les blockchains peuvent être utilisées à de nombreuses autres fins, y compris des applications puissantes qui servent les contrevenants aux sanctions. Elles peuvent servir de plateformes pour des marchés et des marchés secrets, ou d'outils de communication, de commande et de contrôle.

Dans son guide visuel, Reuters définit la nature des blockchains comme: "une base de données partagée sur un réseau d'ordinateurs. Une fois qu'un dossier a été ajouté à la chaîne, il est très difficile de la modifier", à moins que 50% des participants ou plus acceptent de la changer. Pour garantir qu'aucun changement autorisé par moins de 51% des utilisateurs ne se produise et que toutes les copies de la base de données sont identiques, le réseau effectue des contrôles continus et élimine les tentatives frauduleuses de modification du protocole de la chaîne.

Au cours des dix dernières années, après la mise au point de la première crypto-monnaie désormais largement connue sous le nom de Bitcoin, des milliers de crypto-monnaies différentes avec des évaluations très fluctuantes, des objectifs différents, des participants et différents degrés d'anonymat ont vu le jour. La plupart des logiciels utilisés pour les créer sont des logiciels open source, ce qui signifie que tout le monde peut télécharger le code en toute légalité et créer une nouvelle crypto-monnaie.

[1] 1 Go Chang Suk, "North Korea uses Cryptocurrency to Earn Money," MTN, accessed January 23, 2019, http://news.mtn.co.kr/newscenter/news_viewer.mtn?gidx=2018062517065863930

Comment fonctionnent les transactions basées sur la blockchain?

Les crypto-monnaies peuvent être utilement comparées aux paiements par chèques bancaires. Dans une version simplifiée de la vérification de l'identité, les banques contrôlent les signatures des bénéficiaires et des payeurs avant d'autoriser le transfert de fonds.

Pour les transactions de crypto-monnaie, les signatures se composent de codes cryptographiques appelés "clé privée", semblable à un mot de passe. Stocké dans un portefeuille numérique, le code est nécessaire pour signer et recevoir des transactions. Plutôt que les employés de banque vérifient leur authenticité, une équation mathématique met en correspondance les signatures numériques des parties à la transaction tout en les encodant pour que la signature privée ne soit pas révélée.

On pense que les crypto-monnaies sont «anonymes», ou tout au moins «difficiles à repérer». Cette idée fait référence au fait que, pour la plupart des crypto-monnaies, toute personne peut les utiliser sans renoncer à leur identité réelle, à condition toutefois de présenter la signature numérique correcte. De même, il n'existe aucune vérification d'identité dans le monde réel nécessaire pour une personne à qui on peut envoyer des fonds, à condition qu'elle dispose du mot de passe correct.

Cependant, l'anonymat n'est vrai que pour le profane. Des sociétés de sécurité spécialisées ont pu ainsi découvrir des personnes à l'origine de nombreuses transactions à la chaîne, y compris des transactions impliquant des membres d'organisations terroristes.[2] Pourtant, il existe une classe naissante de crypto-monnaies qui se vendent sous couvert d'un anonymat renforcé, ce qui signifie qu'elles utilisent des mathématiques encore plus avancées pour dissimuler l'identité de ses utilisateurs.

Une crypto-monnaie peut être fermée ou ouverte, et les deux ont des implications sur l'abus de sanctions.

[2]https://www.jpost.com/Middle-East/ISIS-Threat/ISIS-other-jihadists-increase-Bitcoin-use-after-fall-of-Caliphate-540079

Enrico Carisch
Phone: (610) 390 9541
Rico.carisch@comcapint.com

www.comcapint.com
110 West 94 Street 2-D
New York, NY 10025

Loraine Rickard-Martin
Phone: (917) 715 2142
loraine.rickard-martin@comcapint.com

	Fermée	Ouverte
Qui peut s'inscrire?	Les utilisateurs doivent être autorisés par la communauté pour effectuer des transactions sur le réseau.	Tout le monde peut effectuer des transactions sur le réseau
Comment sont-elles utilisées?	Pour le fonctionnement d'un système fermé, comme un réseau de banques. La devise n'est probablement pas utile en dehors du système.	Pour les échanges de biens et services, et dans les échanges.
Quelle applicabilité aux abus de sanctions?	Permet aux participants sélectionnés de s'engager sciemment dans des actions sanctionnables sans être découverts.	S'engager dans un anonymat relatif avec des utilisateurs innocents pour obtenir des services, effectuer des transactions ou échanger des crypto-monnaies.

Le marché des crypto-monnaies

Les crypto-coins n'existent pas en tant qu'actif physique. Le terme est utilisé pour décrire une chaîne de code logiciel nommant une valeur spécifique détenue par différentes entités. Ce sont ces chaînes de code à travers lesquelles les transactions peuvent être effectuées.

Actuellement, les estimations de crypto-monnaies individuelles varient, dans le cas de Bitcoin Ether ou Ripple, en milliards de dollars américains. Des dizaines de pièces estimées valent des millions de dollars américains, alors que des centaines d'autres ne valent peut-être que quelques milliers de dollars américains. En 2018, le marché total des crypto-coins a fluctué entre 128,9 milliards et 818,1 milliards de dollars.[3]

L'accès à un réseau de crypto-monnaie n'est possible que pour ceux qui acquièrent de la monnaie, que ce soit par le biais d'échanges spécialisés ou d'autres vendeurs, en minant des pièces de monnaie, ce qui revient à créer des crypto-coins, ou en vendant des biens et services en échange de crypto-monnaie.

Types de crypto-coins et cadres réglementaires

Les réglementations gouvernementales s'appliquent aux crypto-monnaies de manière incohérente et imprévisible. De nombreux pays n'ont même pas évoqué leur existence. D'autres n'ont pas encore décidé s'il s'agissait de valeurs mobilières ou de devises. Aux États-Unis, les mêmes règles relatives aux lois sur les valeurs mobilières s'appliquent aux pièces qui fonctionnent comme un actif ou la propriété d'un bien ou d'un service corporel, par ex. une partie d'une fiducie immobilière. Toutefois, certains cybercoins ne sont pas estimés comme des valeurs s'ils sont considérés comme nécessaires à l'utilisation d'une plateforme blockchain hébergeant des applications Web, par exemple s'ils paient pour un espace de stockage sur un réseau d'ordinateurs partageant une puissance de calcul.

Ethereum était le premier exemple bien connu d'un cybercoin qui n'était pas considéré comme une valeur, mais plutôt comme un «carburant numérique». Ether étant nécessaire à l'utilisation de la plateforme Ethereum, il est traité comme un actif numérique, mais pas comme une valeur. Les personnes utilisent la plateforme Ethereum pour développer des applications utilisant des contrats intelligents, par exemple des éléments de code spécifiant les conditions d'accord entre une ou plusieurs parties. Les utilisateurs expérimentent la création d'applications logicielles à l'aide de ces contrats intelligents, par exemple un code qui exécuterait un service de partage de trajet (semblable à Uber).

[3] https://coinmarketcap.com/charts/

Enrico Carisch
Phone: (610) 390 9541
Rico.carisch@comcapint.com

www.comcapint.com
110 West 94 Street 2-D
New York, NY 10025

Loraine Rickard-Martin
Phone: (917) 715 2142
loraine.rickard-martin@comcapint.com

La communauté des contrats intelligents estime que cet outil numérique représente un moyen important d'éviter les grands conglomérats Internet et de les remplacer par des fragments de code automatisés. Une communauté choisie de programmeurs hautement spécialisés pilote actuellement ces innovations. Le pouvoir de transformation de leurs idées est largement reconnu par de nombreux secteurs. Les autorités de l'immobilier et des cadastres, par exemple, déploient déjà des efforts pour intégrer les contrats intelligents à leurs opérations.

Les contrats intelligents pourraient toutefois aussi servir à des fins illicites, y compris le contournement des sanctions. Par exemple, un contrat intelligent pourrait être utilisé comme preuve cryptée du paiement d'un pot-de-vin à un fonctionnaire en réponse à la délivrance de permis d'exportation, au dédouanement ou à la fourniture de biens sous embargo. Ces contrats intelligents pourraient facilement devenir un moyen de renforcer les alliances entre la RPDC et ses partisans / sympathisants à l'étranger.

Écosystème d'échange de cybercoins

L'achat de cybercoins se fait généralement sur des bourses, qui sont des marchés en ligne auxquels les gouvernements sont de plus en plus soumis à des obligations de déclaration similaires à celles des intermédiaires financiers. Une autre solution consiste à utiliser des marchés numériques tiers (tels que Craigslist) pour trouver des personnes prêtes à acheter ou à vendre des cryptocoins. Ces transactions sont souvent impossibles à suivre et peuvent renforcer l'anonymat de leurs acheteurs ou vendeurs. Bien entendu, les acheteurs et les vendeurs peuvent également se connecter dans l'anonymat le plus total, sans aucun tiers, ni même s'identifier mutuellement pour échanger des chaînes de code pouvant être évaluées à des montants négligeables ou à des millions de dollars mal acquis.
La plupart des bourses de crypto-monnaie sont un marché en ligne avec une entreprise centrale qui achète et vend la ou les devises de son choix. Il existe des centaines de plateformes numériques, dont certaines respectent les lois sur la vérification de l'identité des juridictions respectives. Bien sûr, de nombreuses bourses ne réglementent pas les utilisateurs et sont disposées à traiter des transactions «à risque».[4] Il existe également des échanges Dark Web qui connectent les cybercriminels à des acheteurs de crypto-monnaie, ou à quiconque préférant opérer dans le secret virtuel.

[4] cipher trace q3 report

Il existe une autre classe grandissante d'échanges décentralisée, ce qui signifie qu'une personne ou un groupe de personnes a écrit un logiciel traité au-dessus d'une blockchain, comme Bitcoin, et qu'il coordonne les correspondances entre acheteurs et vendeurs. Ces types d'échanges pouvant fonctionner en l'absence de toute présence physique sont techniquement plus complexes dans la mesure où ils nécessitent une connaissance particulière de la programmation pour la création, la mise à jour et le fonctionnement. Leur réglementation est également plus nuancée, car aucune entreprise centrale n'exige de vérification des utilisateurs.

Le processus de minage de la blockchain

Dans le minage, de nombreux ordinateurs différents peuvent exécuter le même logiciel simultanément pour traiter des chaînes spécifiques de codes logiciels sur le réseau de crypto-monnaie, en concurrence avec d'autres, afin de gagner de nouvelles pièces libérées périodiquement par le protocole qui régit la crypto-monnaie d'origine. Ces ordinateurs tentent de résoudre un nouveau problème mathématique publié parallèlement aux nouvelles pièces potentielles pouvant être minées. En fonction des règles de la crypto-monnaie, certaines d'entre elles nouvellement imprimées apparaîtront dans le portefeuille numérique du gagnant. Les mineurs sont donc incités par une récompense financière à maintenir la sécurité et le registre des transactions.

Les opérations de minage de crypto-monnaie comptent des dizaines, voire des centaines d'ordinateurs modifiés. Étant donné que le minage nécessite la répétition sans fin d'algorithmes à très grande vitesse, la puissance de calcul doit être améliorée avec une carte graphique (GPU) ou un circuit intégré encore plus puissant (ASIC). Ces exigences matérielles sont potentiellement limitées par la forte consommation d'énergie de ces ordinateurs et par la chaleur associée qu'ils émettent.

Il existe de nombreux protocoles différents (logiciels) relatifs au minage qui incitent à gagner les pièces nouvellement créées. La plupart d'entre eux partagent le fait que pour chaque transaction où une personne envoie des fonds ailleurs, l'expéditeur doit payer des frais qui vont aux mineurs de la blockchain.

Enrico Carisch
Phone: (610) 390 9541
Rico.carisch@comcapint.com

www.comcapint.com
110 West 94 Street 2-D
New York, NY 10025

Loraine Rickard-Martin
Phone: (917) 715 2142
loraine.rickard-martin@comcapint.com

Le minage peut être réalisé sur des réseaux majeurs tels que Bitcoin ou l'un des milliers de réseaux plus petits. Pour les nouvelles pièces créées et lorsque l'intérêt public est faible, il est possible de miner des pièces avec moins de puissance de calcul et moins d'électricité.

Abus nord-coréens observés avec les technologies de la blockchain

Il existe cinq différents types d'abus, selon leur application, qui facilitent également les violations des sanctions:

1. L'utilisation de méthodes de piratage traditionnelles et par rançon telles que le DDOS, le phishing, les logiciels malveillants et d'autres attaques d'infrastructure visant les infrastructures à crypto-monnaies.

2. L'emploi du piratage ciblé des échanges de crypto-monnaie pour voler des actifs numériques et les vendre sur d'autres marchés en ligne pour générer des revenus.

3. Le minage légitime de pièces et la négociation de crypto-devises existantes pour générer des revenus à des fins illégitimes.

4. La création de faux comptes de médias sociaux pour un agent ou un homme d'affaires nord-coréen afin de générer un intérêt illégitime dans une entreprise en déguisant la nationalité nord-coréenne et en usurpant d'autres nationalités.

5. La création d'un nouveau système de blockchain de crypto-monnaie ou privée afin de permettre des transactions monétaires difficiles à observer ou d'autres flux de ressources pouvant générer des bénéfices très importants.

1.Piratage traditionnel

Les opérations de piratage classiques ont souvent été rattachées à des auteurs nord-coréens, avec les conséquences suivantes:

	DDOS	Logiciel malveillant	Phishing	Piratage d'infrastructure

Enrico Carisch
Phone: (610) 390 9541
Rico.carisch@comcapint.com

www.comcapint.com
110 West 94 Street 2-D
New York, NY 10025

Loraine Rickard-Martin
Phone: (917) 715 2142
loraine.rickard-martin@comcapint.com

Description de la technologie	Le hacker ferme les sites Web de l'entreprise	Il installe le virus qui détient des fichiers en otage	Vol de mots de passe pour l'utilisateur de comptes institutionnels	Trouve les vulnérabilités dans les serveurs de l'entreprise
Impact commun	Perte d'activité critique	Rançon demandée dans une crypto-monnaie telle que le Bitcoin	Transfert de grandes quantités de fonds	Transfert de fonds importants ou attaques critiques sur des infrastructures telles que les réseaux d'énergie
Objectif de la RPDC	Sabotage	Générer des revenus / Sabotage	Générer des revenus	Générer des revenus / Sabotage

Le 6 septembre 2018, le ministère de la Justice des États-Unis a officiellement inculpé Jin Hyok Park, un pirate informatique nord-coréen, pour avoir perpétré le braquage de la Bangladesh Bank et pour d'autres crimes de piratage financier majeurs, notamment la cyberattaque avec rançon de WannaCry et la violation de Sony Pictures.[5][6] La liste des accusations dans ce cas compte toutes les approches énumérées dans le tableau ci-dessus. Park aurait été membre du groupe Lazarus, un groupe de hackers parrainé par la Corée du Nord.

[5] Catalin Cimpanu, "How US Authorities Tracked down the North Korean Hacker behind WannaCry," ZDNet, accessed January 23, 2019, https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/.

[6] En février 2016, des pirates nord-coréens auraient apparemment obtenu des informations d'authentification légitimes de la banque centrale du Bangladesh pour le système de messagerie interbancaire mondial SWIFT et auraient tenté de transférer 951 millions de dollars des fonds de la banque sur des comptes du monde entier. Cela a permis un vol de 81 millions de dollars — https://www.thecipherbrief.com/kim-digs-cybercrime-coin-sanctions-cant-snatch

Les technologies utilisées dans ces attaques ne reposaient pas sur des technologies de blockchain, mais sur des méthodes d'intrusion de logiciel traditionnelles qui ont évolué au cours de nombreuses années.

2. Piratage d'échanges de crypto-monnaie

Les auteurs ont ciblé les portefeuilles numériques où les échanges de crypto-monnaie stockent les fonds détenus entre les transactions pour les clients. Ces portefeuilles constituent des cibles très lucratives car ils contiennent des quantités importantes de fonds de clients cumulés. Le vol des signatures numériques qui contrôlent ces portefeuilles et la réappropriation des fonds génèrent des gains très importants. Ce revenu numérique est difficile à localiser et peut donc être utilisé pour contourner ou contrevenir au gel des avoirs et à d'autres mesures de sanctions des Nations Unies.[7]

La société de sécurité Group-IB a trouvé des preuves selon lesquelles la RPDC était responsable de 3/4 des piratages d'échanges de crypto-monnaie (représentant un total de ~571 millions de dollars US) entre fin 2016 et l'automne 2018. Il est intéressant de noter que la plus grande attaque attribuée au groupe Lazarus appartenant à la RPDC était d'environ ~534 millions de dollars US d'une nouvelle crypto-monnaie appelée alors le NEM.[8] Les pirates ont envoyé des logiciels malveillants aux employés de la bourse et volé les mots de passe du portefeuille.

3. Le minage

Les intrusions dans les opérations de minage de crypto-monnaie sont perpétrées de plusieurs façons: Les pirates peuvent identifier les vulnérabilités dans les règles du protocole (logiciel) nécessaires au minage, et réaffecter des pièces à de nouveaux portefeuilles.

[7] https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html
[8] https://www.group-ib.com/resources/threat-research/cryptocurrency-exchanges.html

Enrico Carisch
Phone: (610) 390 9541
Rico.carisch@comcapint.com

www.comcapint.com
110 West 94 Street 2-D
New York, NY 10025

Loraine Rickard-Martin
Phone: (917) 715 2142
loraine.rickard-martin@comcapint.com

Une autre méthode consiste à dominer la blockchain des mines en prenant le contrôle de 51% du réseau, leur permettant ainsi de créer des transactions frauduleuses et de contrôler le portefeuille des mineurs.[9] On ignore si les nord-coréens comptent parmi les auteurs qui ont réussi de telles intrusions dans les activités de mines.[10]

Selon le rapport d'août 2018 de la Korean Development Bank, les Nord-Coréens ont tenté de miner des Bitcoins à grande échelle entre mai et juillet 2017, mais ils n'ont peut-être pas réussi à produire des quantités significatives de pièces.[11] Le manque de rentabilité peut avoir été causé par la forte consommation d'énergie inhérente au crypto minage et par la concurrence croissante entre les mineurs.

Depuis, la Corée du Nord s'appuierait sur Monero, une crypto-monnaie mieux protégée par l'anonymat qui peut être minée à l'aide d'un ordinateur classique plutôt que d'un modèle puissant prévu pour le minage. Les pièces gagnées peuvent ensuite être échangées contre des biens ou converties en devises fiduciaires.

Le rapport de la Korean Development Bank mentionne également une société nord-coréenne appelée «Chosun Expo» qui développe une plate-forme de tarification facilitant la répartition et le commerce de bitcoins.[12]

En raison des coûts énergétiques des mines, les Nord-Coréens semblent préférer pirater des cryptomonnaies plutôt que de les miner. Le Financial Security Institute basé en Corée du Sud a signalé l'existence du groupe de piratage Andariel de la RPDC qui s'est introduit à l'été 2017 dans le serveur d'une société sud-coréenne et l'a utilisé pour miner 70 Monero (d'une valeur comprise entre 25 000 $ et 50 000 dollars US).[13] Russian/UK Kaspersky Lab et Alien Vault ont également trouvé un logiciel destiné à miner Monero pour envoyer des fonds à l'Université Kim Il Sung à Pyongyang, en Corée du nord.[14] Les preuves montrent qu'il s'agissait probablement d'un prototype de logiciel malveillant

---

[9] https://blog.theabacus.io/the-verge-hack-explained-7942f63a3017
[10] https://www.bleepingcomputer.com/news/cryptocurrency/hacker-uses-exploit-to-generate-verge-cryptocurrency-out-of-thin-air/
[11] Min Gwan Kim, "Weekly KDB Report - Cryptocurrency Use in North Korea," August 27, 2018.
[12] Min Gwan Kim, "Weekly KDB Report - Cryptocurrency Use in North Korea," August 27, 2018
[13] https://www.bloomberg.com/news/articles/2018-01-02/north-korean-hackers-hijack-computers-to-mine-cryptocurrencies
[14] https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html

pouvant être installé sur des ordinateurs piratés afin de pouvoir miner Monero secrètement en arrière-plan.[15]

4. Usurpation d'identité de propriétaires d'entreprise non nord-coréens ou utilisation des médias sociaux pour dissimuler les origines de leurs bienfaiteurs

Dans l'exemple de Park Jin Hyok, (déjà cité sous le paragraphe 1. Piratage traditionnel), l'Office of Foreign Assets Control du département du Trésor des États-Unis fait référence à un certain nombre de pseudonymes, dont "Kim Hyon Woo". Sous ce nom, Hyok a mis en place plusieurs comptes de médias sociaux et Gmail et des éléments de preuve ont montré qu'ils étaient utilisés pour les piratages du groupe Lazarus. Les preuves de ces connexions sont basées, notamment, sur l'adresse IP ou les adresses électroniques des opérations de piratage du groupe Lazarus et de leurs victimes, toutes reliées également au gouvernement de la Corée du Nord.[16]

On soupçonne également que, lors de la vague spéculative de 2017-2018, lorsque les évaluations de Bitcoin, d'Ether et de nombreuses autres crypto-devises ont explosé, une augmentation du nombre de faux comptes de médias sociaux usurpant l'identité d'entreprises de la blockchain aurait pu être liée à des promoteurs de fausses pièces ou de l'Initial Coin Offerings. Les ICO pour les nouvelles crypto-monnaies génèrent normalement le plus d'argent grâce à une idée nouvelle si des leaders reconnus du secteur en font la promotion. Ainsi, si des investisseurs inconnus croient à ces fausses associations, le système peut générer plus d'argent. Une investigation approfondie est nécessaire pour découvrir s'il existe des liens avec la RPDC.

L'absence de règles et de restrictions dans le monde réel pour les procédures de vérification d'identité avec les utilisateurs de médias sociaux est l'une des raisons pour lesquelles de tels systèmes d'usurpation d'identité peuvent réussir. Bon nombre des revenus de ces plateformes augmentent avec l'augmentation du nombre d'utilisateurs. Par conséquent, les plateformes telles que LinkedIn, Facebook ou Twitter ne sont pas incitées à imposer des contrôles d'identification rigoureux et fiables à leurs utilisateurs,

[15] https://www.alienvault.com/blogs/labs-research/a-north-korean-monero-cryptocurrency-miner
[16] https://www.federalregister.gov/documents/2018/09/12/2018-19785/notice-of-ofac-sanctions-actions

ouvrant ainsi la porte à des contrevenants de sanctions potentiels se cachant derrière de faux comptes d'utilisateurs.

Outre l'utilisation des médias sociaux pour dissimuler les véritables bienfaiteurs, il existe une tendance référencée selon laquelle les autorités nord-coréennes changent de nom et tirent parti de la traduction du coréen vers l'anglais, créant ainsi une liste déroutante d'identités et de responsabilités pour les actions.[17]

5. Création de nouvelles crypto-monnaies ou de blockchains privées

Il existe deux cas référencés de ressortissants de la RPDC qui ont créé des crypto-actifs numériques par le biais d'organisations internationales de propriété dans un but lucratif, dénommés Marine Chain et Interstellar (également appelé Stellar ou HOLD) et renommés en pièce Huzu.[18] Marine Chain était un collecteur de fonds, ou un financement participatif, d'un nouveau cryptocoin dirigé par un PDG de Singapour, le capitaine Jonathan Foong Kah Keong. Selon la société de sécurité Recorded Future, il est affilié à d'autres sociétés singapouriennes qui ont soutenu les Nord-Coréens dans leurs efforts de contournement des sanctions depuis au moins 2013. Ces opérations illicites ont été coordonnées par des facilitateurs nord-coréens basés à Singapour.[19]

Normalement, une ICO lève des fonds en vendant une idée future comprenant le cryptocoin et les nouvelles capacités financières sur lesquelles il va innover. Par exemple, Marine Chain a prétendu qu'il s'agissait de jetons de navires, ce qui signifie qu'il créait une pièce de monnaie cryptée qui représentait la propriété des entreprises maritimes.

Dans les deux cas, ceux qui sont à l'origine du système n'ont jamais rien développé au-delà de l'actif lui-même, ce qui signifie qu'ils n'ont pas réellement connecté ces actifs au marché maritime. Au lieu de cela, ils ont ainsi empoché les fonds destinés au régime de la RPDC. Il semble actuellement que la seule intention de créer cet actif soit le profit à court terme. Cependant, il souligne les possibilités de créer une monnaie basée sur

---

[17] Min Soo Kang, "Why Do North Korean Official Like Aliases?," KBS, accessed January 28, 2019, http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=056&aid=0010665129&sid1=001

[18] https://www.recordedfuture.com/north-korea-internet-usage/

[19] https://www.recordedfuture.com/north-korea-internet-usage/

une blockchain qui pourrait en réalité s'appuyer sur des biens et services tangibles comme moyen de contourner les sanctions.

Ainsi, il n'est pas impossible d'imaginer que la RPDC crée sa propre crypto-monnaie qui pourrait être utilisée pour contourner les sanctions, et ce sans que les autres parties aient connaissance du propriétaire de la RPDC qui se trouve derrière le système / la devise.

Le projet général a également touché d'autres personnes, notamment à des fins élogieuses. Un correspondant du Seoul Economic Daily a récemment écrit un article sur l'utilité d'une monnaie numérique collaborative nord-sud-coréenne pour créer une «monnaie neutre», affirmant qu'elle pourrait accroître la transparence, l'efficacité et les relations.[20] Il reste à voir s'il y a plus d'engouement autour de ce scénario.

Meilleures pratiques pour les responsables de l'application des sanctions

Jusqu'alors, dans l'histoire des technologies numériques, la mise en œuvre des sanctions a été réactive, tardive et donc peu efficace. Les sanctions imposées à la sphère numérique doivent tenir compte des abus en cours, qui s'aggraveront sans doute au fur et à mesure que les compétences technologiques des contrevenants se renforceront.

La principale priorité des meilleures pratiques en matière d'activités cybernétiques demande à ce qu'elles soient traitées comme elles le seraient dans le monde réel. En fin de compte, il n'y a pas de différence entre le blanchiment d'argent avec des actifs conventionnels ou cyber.

L'anonymat et la nouveauté de ces technologies renforcent le potentiel de pratiques trompeuses et d'actions risquées des entités déjà sanctionnées d'une part et de nouveaux acteurs menaçants d'autre part. En raison des risques accrus, les pratiques d'audit préalable doivent être encore plus fermes. Les acteurs qui préfèrent opérer au

[20] Seoul Economic Daily, "Cryptocurrencies Will Facilitate North-South Relations," Seoul Economic Daily, accessed January 23, 2019, http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=011&aid=0003491320&sid1=001.

sein de réseaux d'information situés sur des blockchains ou hautement cryptés s'écartent des pratiques en vigueur dans l'industrie et des obligations de rapport existantes. Par conséquent, une vigilance accrue est requise pour toute entité engagée dans des transactions relatives aux armes ou aux opérations financières, dans les transports maritimes ou aériens, ainsi que dans les interactions avec des travailleurs ou des diplomates nord-coréens pour lesquels l'utilisation de plateformes à la pointe de la technologie est suggérée. Les mesures recommandées:

- Insister sur la divulgation complète des pièces d'identité vérifiables, des objectifs de la transaction proposée et de toute autre information pertinente qui serait prise en compte dans une transaction réelle.
- Clarifier la raison d'être de l'activité proposée pour s'assurer que toutes les étapes économiques servent des objectifs raisonnables, logiques et légitimes.
- Lors de la création de nouvelles cyber entreprises, il convient de contrôler toutes les parties impliquées, de s'assurer que le financement et les capitaux, versés sous forme de monnaie numérique ou non, ne sont pas liés à une violation de sanction ni à des actifs supposés être bloqués;
- Imposer des exigences de divulgation à toute entreprise ou entreprise basée sur la technologie de la blockchain pour authentifier la légitimité d'actifs, de contenus de portefeuilles numériques ou d'objectifs de contrats intelligents;
- Insister sur le fait que les institutions financières et les entreprises, y compris les émetteurs et les émetteurs de crypto-monnaie, doivent bénéficier d'une protection de la sécurité des réseaux, à commencer par l'éducation et les règles relatives aux logiciels malveillants / phishing / mots de passe afin de mieux protéger le système financier national contre les intrusions non autorisées.
- Imposer des obligations d'intégrité aux opérateurs d'installations de cloud computing afin d'optimiser la protection contre les intrusions de logiciels malveillants.

Pour les particuliers, les entreprises ou les entités déjà sous sanctions de l'ONU:

- Bloquer tout commerce de produits, composants ou technologies soumis à un embargo;

Enrico Carisch
Phone: (610) 390 9541
Rico.carisch@comcapint.com

www.comcapint.com
110 West 94 Street 2-D
New York, NY 10025

Loraine Rickard-Martin
Phone: (917) 715 2142
loraine.rickard-martin@comcapint.com

- Bloquer les comptes financiers et les portefeuilles numériques, et archiver les rapports de transactions suspectes, le cas échéant;
- Refuser toutes les activités numériques ou l'accès aux comptes sur les plateformes technologiques numériques, y compris les médias sociaux, les marchés, les applications, le cloud computing et la messagerie électronique, s'il existe des indications que ces activités peuvent contribuer à la violation de sanctions.